INL/CON-06-01212
PREPRINT

A Comparison of the Safety Analysis Process and the Generation IV Proliferation Resistance/Physical Protection Assessment Methodology

International Conference on Probabilistic Safety Assessment and Management

T.A. Bjornard
M.D. Zentner

May 2006

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

A COMPARISON OF THE SAFETY ANALYSIS PROCESS AND THE GENERATION IV PROLIFERATION RESISTANCE/PHYSICAL PROTECTION ASSESSMENT METHODOLOGY

M.D. Zentner
Pacific Northwest National Laboratory

T.A. Bjornard, Ph.D.
Idaho National Laboratory

ABSTRACT

The Generation IV International Forum (GIF) is a vehicle for the cooperative international development of future nuclear energy systems. The Generation IV program has established primary objectives in the areas of sustainability, economics, safety and reliability, and Proliferation Resistance and Physical Protection (PR&PP).

In order to help meet the latter objective a program was launched in December 2002 to develop a rigorous means to assess nuclear energy systems with respect to PR&PP. The study of Physical Protection of a facility is a relatively well established methodology, but an approach to evaluate the Proliferation Resistance of a nuclear fuel cycle is not. This paper will examine the Proliferation Resistance (PR) evaluation methodology being developed by the PR group, which is largely a new approach and compare it to generally accepted nuclear facility safety evaluation methodologies.

Safety evaluation methods have been the subjects of decades of development and use. Further, safety design and analysis is fairly broadly understood, as well as being the subject of federally mandated procedures and requirements. It is therefore extremely instructive to compare and contrast the proposed new PR evaluation methodology process with that used in safety analysis. By so doing, instructive and useful conclusions can be derived from the comparison that will help to strengthen the PR methodological approach as it is developed further.

From the comparison made in this paper it is evident that there are very strong parallels between the two processes. Most importantly, it is clear that the proliferation resistance aspects of nuclear energy systems are best considered beginning at the very outset of the design process. Only in this way can the designer identify and cost effectively incorporate intrinsic features that might be difficult to implement at some later stage. Also, just like safety, the process to implement proliferation resistance should be a dynamic, iterative process that continually evolves with the design.

INTRODUCTION

The Generation IV International Forum (GIF) is a cooperative international program for developing future-generation nuclear energy systems. Important elements in the GIF program are four primary goals for ensuring sustainability, economics, safety and reliability, and proliferation resistance and physical protection (PR&PP).

In response to the GIF Program Goals, a process to develop an evaluation methodology to assess nuclear energy systems with respect to PR has been on-going since December 2002. A similar process is underway by a GIF working group on Risk and Safety (RSWG) to assure a harmonized approach on long-term safety, risk, and regulatory issues in development of the proposed GIF nuclear energy systems. The entire energy system must be evaluated and compared, from the front end of the fuel cycle through the reactor system to spent fuel storage or reprocessing and finally waste disposal.

While the safety and reliability analysis process used in nuclear facilities is a mature technology with a variety of analytical techniques available to be adapted to the needs of the Generation IV program, the PR assessment methodology is still under development. We propose that a critical examination of elements of the accepted safety and reliability evaluation process as it is currently practiced and a comparison with the PR assessment process can provide important insights, both to the PR development team as well as to potential users of the PR assessment methodology.

Accordingly, in this paper we first describe the process for the Hazard and Accident Analyses performed during a U.S. Department of Energy Documented Safety Analysis (DSA). We then contrast that with a proposed process

for application of the PR Assessment Methodology currently under development. Similarities and differences in the two methodologies are explored, and insights and conclusions are presented.

A SUMMARY OF THE PROCESS FOR PERFORMING DOCUMENTED SAFETY ANALYSIS

The United States Code of Federal Regulations (10 CFR 830) establishes requirements for performing a facility safety analysis and assuring safe operation of the facility. The process and result of meeting these requirements is called the Documented Safety Analysis (DSA)[1] [1-3].

Key tasks in establishing the basis for the facility safety analysis are the hazard and accident analyses that are performed to identify specific controls and improvements important for overall safety management. Consequence and likelihood estimates obtained during this process form the bases for establishing the level of detail and control needed for minimizing the risk to workers and the public. The result is a documented safety basis which establishes the controls needed to maintain safe operation of a facility over its lifetime

Figure 1 shows a methodological outline for the safety analysis process.

CHALLENGES >> SYSTEM RESPONSE >> OUTCOMES
Accident Initiators *Systems Analysis* *Consequences*

Figure 1 Safety Analysis Methodological Approach

In this process, the challenges to a facility are ***accident initiators*** that can result from stochastic failures within the system, from personnel errors, or from external natural hazards. The ***system response*** would be determined using a safety analysis approach to evaluate the facility response to the accident initiators. The ***consequences*** (outcomes) are health and safety descriptors (deaths, core damage, economic loss, etc.).

Safety Analysis

The safety analysis process begins with a preliminary hazard categorization of the facility, identifying material located in the facility and determining potential consequences if an accident resulting in a radiological/biological/chemical (depending on the type of facility) release should occur.. A graded approach is used depending on whether the consequences of accidents at the facility have a possibility of a significant offsite effect (Category 1 facilities), a significant onsite event (Category 2 facilities), or significant localized consequences (Category 3 facilities). Next, hazard assessment and accident analyses are performed. The level of detail involved in the safety analysis depends on the hazard category. Figure 2 demonstrates this by comparing the level of analytical detail required depending on the facility category. As the safety analysis proceeds, the facility categorization is revisited and may be changed. This iterative process continues until the analysis is complete and no further changes are taking place.

Hazard Analysis

The Hazard Analysis process consists of collecting and integrating four interrelated sets of information:

- Hazardous Material Quantity, Form, and Location
- Energy Sources and Potential Initiating Events
- Candidate Preventive Features
- Mitigative Features.

The Hazard Analysis identifies the maximum hazardous material inventory permitted to be processed or present in specific locations in the facility. Material form, which includes forms such as powder, metal (large pieces or shavings), sludge, gas, solid waste, or liquid, is then determined. Locations are specified, indicating the part of the building, glovebox, or process line in which the material is present. Next, potential energy sources and potential initiating events that could affect the hazardous material and lead to a release of material or other occurrence are identified. Finally, any structure, system, or component that serves to prevent the release of hazardous material in an accident scenario is identified. Preventive features may include passive barriers such as piping, material containers, material cladding, gloveboxes, or facility structures as well as systems or components such as pressure relief valves,

[1]This paper primarily addresses the process for developing DSA's for non reactor nuclear facilities.

monitoring systems for material concentrations with automatic actions to stop or isolate the process, or dilution systems to control explosive or flammable mixtures.

Accident Analysis

In the "Graded" analysis approach, the effort expended in performing an accident analysis is a function of the hazard and the complexity of a particular process, and builds upon the Hazard Analysis already performed. A wide variety of analysis techniques is available, and a primary objective of the graded approach is to select and apply a rigorous analysis technique that will provide sufficient detail to assess each postulated accident or failure, the resulting consequences, and all means of prevention or mitigation.

The accident analysis approach consists of four distinct elements as highlighted in Figure 2:

- Release Mechanism Analysis,
- Sequence Selection,
- Engineering Analysis, and
- Consequence Analysis.

The release mechanism element identifies the vulnerabilities in the structures, systems, and components that could create conditions for or cause releases of hazardous material. The results of the step are a comprehensive set of potential accident sequences which provide the basis for the next element, sequence selection. In the sequence selection process, the critical step of selecting the postulated accident sequences used in the remainder of the accident analysis process is performed. Non-significant sequences are culled out and removed from further consideration. The engineering analysis step identifies the physical relationships among the systems, structures, and components, and the release mechanisms for the selected sequences. This is a critical part of the analysis because it connects the facility, the hazardous material, and the physical conditions during the postulated accident. The final element in the accident analysis is consequence analysis. This step evaluates the effect of the postulated accident on the workers, the public, and the environment.

Safety Analysis Results

The safety analysis process is performed to identify specific controls and improvements important for overall safety management, to ensure safe operation of a facility over its lifetime, and for the identification of facility modifications needed to ensure safe operation. Consequence and likelihood estimates obtained during this process form the bases for establishing the level of detail and control needed based on minimizing the risk to workers and the public. Specific results include identification and development of:

- Safety-class Structures, Systems, and Components
- Safety-significant Structures, Systems, and Components
- Technical Safety Requirements
- Necessary Facility modifications

Safety-class structures, systems, and components are those structures, systems, and components, including portions of process systems, whose preventive and mitigative function is necessary to limit radioactive hazardous material exposure to the public. Safety-significant structures, systems, and components are those structures, systems, and components that are not designated as safety-class SSCs but whose preventive or mitigative function is a major contributor to defense in depth and/or worker safety. Technical safety requirements (TSRs) are the limits, controls, and related requirements necessary for the safe operation of a nuclear facility and, as appropriate for the work and the hazards identified in the documented safety analysis for the facility, includes safety limits, operating limits, surveillance requirements, administrative and management controls, use and application provisions, and design features, as well as a bases appendix. As a result of performing the Safety Analyses, vulnerabilities will be identified and changes to facility structures, systems, and components will be required. As these changes are made, the process must be revisited to ensure no new, unidentified failures or hazards have been introduced.

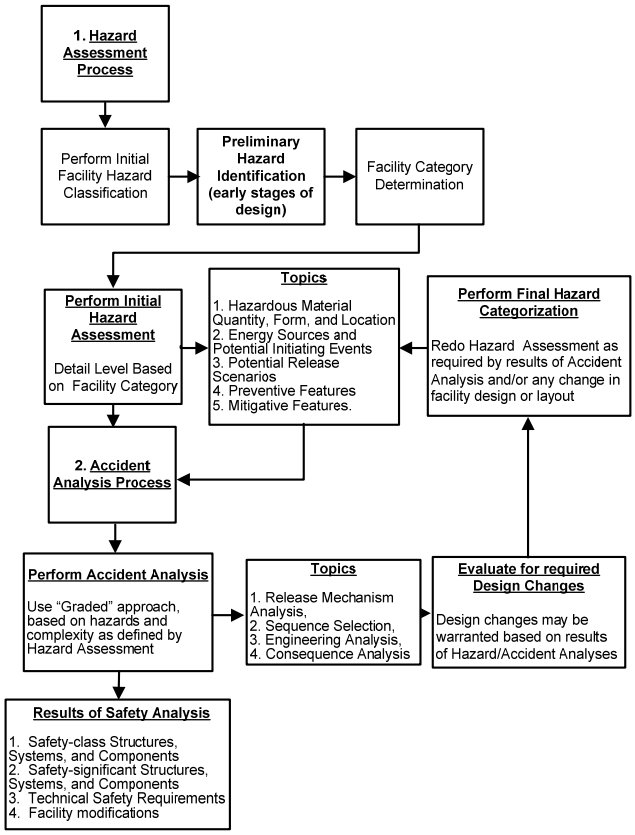

Figure 2 Safety Analysis Overview

Noteworthy is the fact that for a new facility, the safety analysis process is an integral step of the design process, and operates in an iterative fashion. Safety analysis results are used to understand the relative strengths and weaknesses of the system from a safety point of view. As changes and improvements are identified they are fed for consideration back into the design process.

THE PROLIFERATION RESISTANCE ANALYSIS PROCESS

Proliferation Resistance Background

The PR methodology being developed may be used for two purposes. First, it is intended to be used in the comparative assessment of nonproliferation robustness of alternative nuclear energy systems or fuel cycles. Additionally, it can be used during the design process of a single nuclear energy system, or facility, for purposes of enhancing the proliferation resistance and physical security of the system.

The PR&PP Expert Group of the GIF has adopted the definition for Proliferation Resistance as established by the International Atomic Energy Agency:

> ***Proliferation resistance*** is that characteristic of a nuclear energy system that impedes the diversion or undeclared production of nuclear material, or misuse of technology, by the Host State for purposes of acquiring nuclear weapons or other nuclear explosive devices.

The proliferation resistance of a nuclear energy system results from the combined, integral effect of a large number of characteristics and processes, including those of both ***intrinsic features*** (engineering options that include basic characteristics and design based features that are usually very robust and difficult to change) and ***extrinsic measures*** (Institutional Arrangements or Host State actions, like treaties or safeguards activities***)***. Some intrinsic features serve to facilitate the implementation of extrinsic measures (e.g. adding a wall in a facility that would facilitate the containment and surveillance step of nuclear material safeguards).

The Basic Approach

It should be noted that this paper was written in order to present aspects of the proliferation resistance analysis process to the safety analysis community, and some modest license has been taken to use concepts and terms more familiar to that audience. The reader looking for an in-depth explanation of the PRPP evaluation methodology itself is referred to the PR&PP methodology report [4].

The methodological approach for PR evaluation methodology is illustrated conceptually in Figure 3. As with safety analysis, for a given nuclear energy system a set of ***challenges*** is defined, the ***response*** of the system is assessed and ***outcomes*** are determined. Relevant characteristics of the nuclear energy systems; intrinsic and extrinsic, technical and institutional are considered in determining the system's response to proliferation threats.

The proliferation ***challenges*** to the system (by potential proliferant States) are called 'threats', and include nuclear material diversion, undeclared production of nuclear materials, abrogation using declared facilities and materials, and the construction and operation of completely separate, clandestine facilities. As with safety analysis, the response of the system and potential outcomes are dependent on the nature of the identified threats.

The PR assessment involves decomposition of the nuclear system into elements[2], identification of potential targets[3] within each of those system elements, and identification and compilation of all potential sequences of events (called 'pathways') that could result in successful proliferation. The ***outcomes*** of the system response are assessments that integrate the sub-elements of the analysis and interpret the results. GIF has adopted the term 'measures' to describe outcomes.

CHALLENGES >> SYSTEM RESPONSE >> OUTCOMES
Threats *PR Assessment* *Measures*

Figure 3 The Basic Methodological Approach for PR Assessment

Proliferation Resistance Assessment

An initial target assessment should be made of the facility, preferably at an early stage of the design, identifying the material contained there, evaluating the facility technology, and performing a preliminary examination of the safeguards that may be required. Then, just as in the nuclear safety process, a graded approach to the PR analysis process should be established, whereby those facilities containing significant quantities of sensitive material or technologies of interest to potential proliferants would receive more detailed analysis.

Figure 4 outlines a proposed approach to the process of assessing proliferation resistance that can be performed in parallel to the nuclear facility safety analysis as described above. The first step is the Target Analysis that identifies the materials or processes of interest. The second step is the Pathway Analysis that explores how the materials or processes could be diverted or misused. The following discussion describes the process steps in a little more detail.

Target Assessment

The target assessment process consists of identifying collecting and integrating the following types of information about the facility

- Material Quantity, Quality, Form, and Location
- Facility Technology
- Proliferation Resistant Features

Material Quantity, Quality, Form, and Location

In the PR methodology, Material Quality is defined as that degree to which the characteristics of the material affect its utility for use in nuclear explosives. This step identifies the quality of the material present at different locations in the facility, and identifies the maximum inventory permitted to be processed or present in specific locations.

[2] A facility, part of a facility, a collection of facilities, or a transportation system within the identified nuclear energy system.
[3] Proliferation resistance targets are nuclear material and processes to be protected from PR threats of diversion and undeclared production.

Material form is assessed to identify potential forms such as powder, metal (large pieces or shavings), sludge, gas, solid waste, or liquid. Locations are specified, indicating the part of the facility, reactor, building, glove box, or process line in which material is present.

Facility Technology

Each nuclear fuel step[, from mining, conversion, enrichment, fuel processing, irradiation in a nuclear reactor, spent fuel storage, transportation and reprocessing presents a different proliferation challenge, and those challenges may even vary among facilities using the same technology. This step identifies and defines the technology for use in the Pathway Analysis.

Proliferation Resistant Features

Each nuclear fuel cycle and component facility contains intrinsic features and/or extrinsic measures that contribute to its proliferation resistance. Included are such things as physical barriers, safeguards systems, material form and quantity, structures, guard forces, and secure facilities. In this step, these features are identified and described for use in the pathway analysis. This may build on the information found in the material assessment step.

Pathway Analysis

The PR Expert Group has chosen the term 'pathway' to describe the sequence of events or actions that could potentially be followed by a State in order to achieve a proliferation objective.

In proliferation resistance analysis, a full pathway is composed of a series of segments and can be divided into three major stages:

- **Acquisition**: Activities carried out to acquire nuclear material in any form, starting with the decision to acquire the material and ending with the availability of the material.
- **Processing**: Activities carried out to convert the nuclear material obtained in the Acquisition stage into material ready for use in a nuclear weapon. Processing may include such activities as irradiation of targets, plutonium separation, uranium enrichment, and conversion of oxides or fluorides to metal.
- **Fabrication:** Activities carried out to manufacture and assemble one or more nuclear explosive devices.

In this case, the "Graded" analysis approach represents the effort expended in performing the PR assessment as a function of the targets and the complexity of a particular process, and builds upon the Target Assessment already performed. A wide variety of analysis techniques[4] are available and a primary objective of the graded approach is to select and apply a rigorous analysis technique that will provide sufficient detail to assess each postulated proliferation pathway. Just as in the case of safety analysis, it is of vital importance in PR analysis that ***all*** possible pathways are identified and analyzed. This means that substantial rigor, and perhaps also very significant effort, must be invested in the process of identifying all possible pathways.

Just as in the case of safety analysis, it is of vital importance in PR analysis that ***all*** possible pathways are identified and analyzed. This means that substantial rigor, and perhaps also very significant effort, must be invested in the process of identifying all possible pathways.

Proliferation Resistance Assessment Results

The results of the PR assessments may be presented in terms of fairly simple metrics that permit identification of the strengths and weaknesses of a system or facility from the point of view of proliferation resistance. These assessments are performed to assess the degree of proliferation resistance of a facility, and to identify intrinsic features and extrinsic measures that can result in:.

- Enhanced Proliferation Resistant Materials, Processes and Facilities
- Enhanced Facility Safeguards
- System and Facility Design Improvements

Following is a brief discussion of each.

Enhanced Proliferation Resistant Materials, Processes and Facilities

One of the four goals of the GIF program is that future nuclear energy systems must remain a very unattractive and least desirable route for obtaining weapons-usable nuclear materials. The results of the PR analysis will provide

[4] For example, Event Trees and Fault Trees, Markov Analysis, Multiple Attribute Utility Analysis, etc

feedback into the design process to cost effectively strengthen the system, while also providing a systematic measure that the objective is met. The application of PR analysis during the design will help to incorporate PR intrinsic features in a cost effective manner.

Enhanced Facility Safeguards,

The detailed analysis will provide a structured approach for evaluating safeguards, identifying potential weaknesses or alternative approaches, and provide a basis for improving and enhancing existing facility safeguards. In the case of meeting fixed safeguards requirements, such as in international safeguards, the PR analysis can be useful in identifying and incorporating intrinsic features that simplify the safeguards process and make it more cost effective (for example, trading an intrinsic improvement for effort otherwise required as an extrinsic, operational measure).

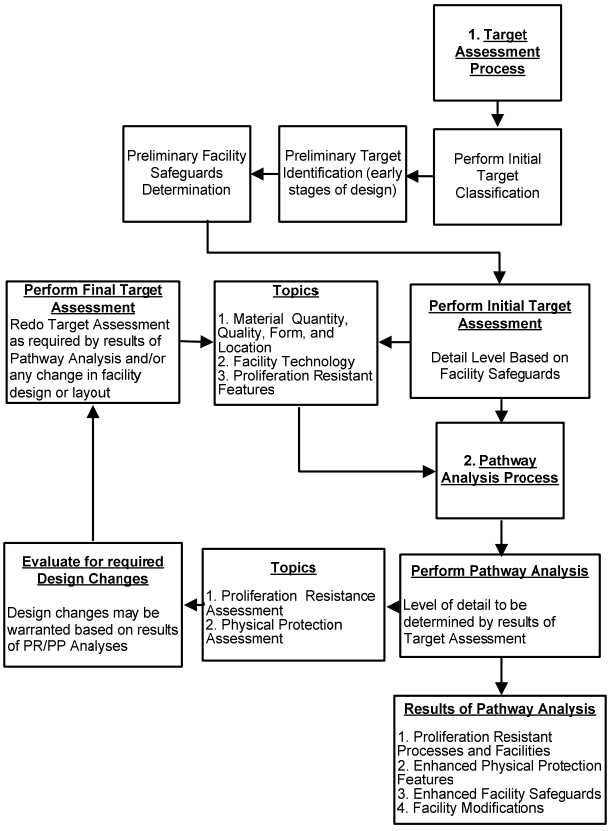

Figure 4 Proliferation Resistance Assessment Process

System and Facility Design Improvements

Incorporation of the PR analysis in the design process of a nuclear facility, or energy system provides the basis for informed, cost-benefit based decisions about incorporating specific intrinsic features and/or extrinsic measures to enhance proliferation resistance. By including this assessment in the design process, before construction has begun, the PR methodology protects the full flexibility to assess design trade-offs at the most fundamental level.

Comparison of Proliferation Resistance and Safety Analysis Processes

Figure 5 below compares the proposed PR assessment and Documented Safety Analysis processes. If it is decided to implement the PR analysis methodology as a parallel process, it can be seen that at various stages of facility design and development related activities could occur. It is reasonable to assume that if an early target assessment would be performed, the appropriate time would be during the hazard assessment process. During the initial facility hazard classification process, the facility hazard category is determined (among other factors such as

potential energy sources) based on the maximum amount and form of material present and the technology involved. This information would be of use to categorize the facility from an available "targets" point of view.

The process of assessing potential targets could be done in a fashion similar to that of the hazard assessment. During the hazard assessment process the maximum quantity of material involved, including its material form and possible locations is established. Potential initiating events that could affect the hazardous material and lead to a release are identified. Structures, systems, or components that serve to prevent the release of hazardous material in an accident scenario are described. Structures, systems, or components that serve to mitigate the consequences of a release of hazardous materials in an accident scenario are identified. There are obvious parallels in this process to identifying and classifying targets both for the physical protection and proliferation resistance assessment process.

Additionally, at this stage the evaluation required to determine potential safeguards that would be required could be done. Once the proliferation related targets have been documented, necessary facility safeguards will be more easily determined.

Finally, the pathway assessment could be done in parallel with the Accident Analysis. The amount and level of detail required for each is similar, and changes in facility structure as a result of either analysis could result in changes in analysis conclusions.

This approach described here reflects a time and cost-efficient way to combine PR Assessments with required Safety Analyses.

Conclusions

The PRPP Evaluation Methodology being developed as part of the GIF program follows the same basic three step structure as the process for performing a Documented Safety Analysis under DOE requirements. In both cases the methodology 1) seeks to draw conclusions about system performance from analyzing the system response to challenges acting against the system and 2) In the case of safety analysis, one is concerned with accident initiators, potential accident sequences, the analysis of the system's response under the postulated sequences, and the consequences of the postulated sequences in terms of defined criteria. Safety analysis is a mature and fairly broadly understood process, so this process was used as the model from which the process for applying the PRPP methodology was constructed for this paper.

In the case of the process for PR evaluation the analysis concerns itself with examining the response of the nuclear energy system (or facility) to action sequences that might be carried out by a proliferant State for purposes of acquiring a nuclear explosive. Just as in the case of safety analysis, it is crucial that all possible pathways are identified and evaluated, in order to obtain a valid conclusion about the degree of proliferation resistance offered by the system.

Several important insights resulted from juxtaposing and comparing the safety analysis and PR processes:

- Safety design is a dynamic, progressive, iterative process where the safety analysis commences with the initial stages of the design process, and feeds back into the design in an iterative fashion. The design is not considered complete until an acceptable safety analysis result is achieved.
- Proliferation resistance of a facility or system reflects the combined, integral effect of a number of basic characteristics, intrinsic features and extrinsic measures. Since intrinsic features can only be cost-effectively implemented if they are included as part of initial construction, it is obvious that the PR analysis should begin with commencement of the basic design process.
- There are almost always trade-offs associated with the implementation of any given design feature, whether for safety, or for nonproliferation. The application of a systematic, rigorous methodology for PR analysis, during the design process provides a useful and reasonable means for evaluating proliferation resistant design features, and making informed, cost-benefit decisions about design trade-offs, such that a reasonable balance can be achieved between the major competing design considerations.
- This brief discussion shows that parallels between the universally accepted safety analysis process and the proliferation resistance methodology under development do exist. In addition, it demonstrates that the two different types of analyses could be done in an interactive fashion, sharing information and coordinating efforts in a cost effective and efficient manner.

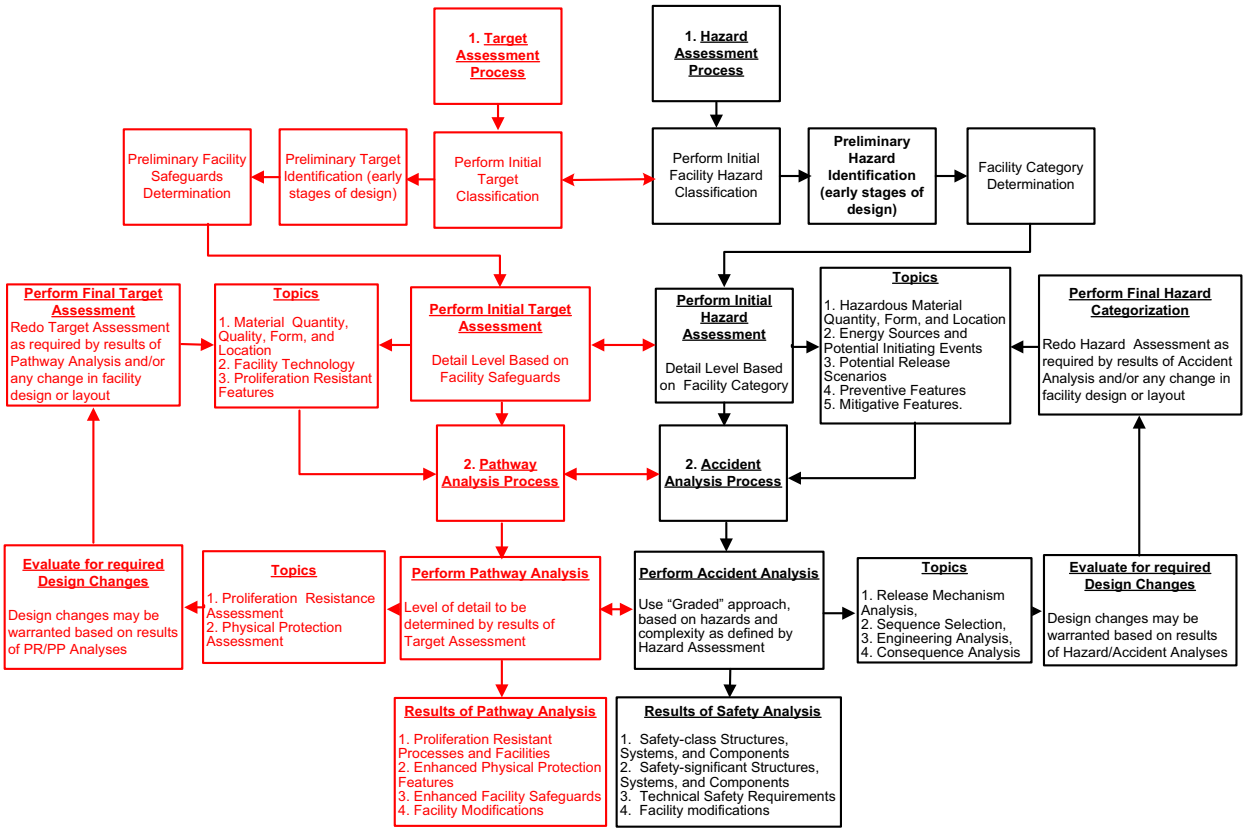

Figure 5 Comparison of the proposed Proliferation Resistance and Safety Analysis Processes

REFERENCES

1. DOE-STD-3009-94, *Preparation Guide for U.S Department of Energy Non-reactor Nuclear Facility Documented Safety Analyses*
2. DOE-STD-1027-92, *Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23*
3. 10 Code of Federal Regulations 830 Appendix A
4. *Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy Systems*, Proliferation Resistance and Physical Protection Evaluation Methodology Expert Group, Revision 4 , April 2006
5. *Proliferation Resistance Fundamentals for Future Nuclear Energy Systems*, STR-332, International Atomic Energy Agency, December 2002